# Realizing Homomorphic Secure Protocols through Cross-Layer Design Techniques( Abstract_要旨 )

AUTHOR(S):

Bian, Song

CITATION:

Bian, Song. Realizing Homomorphic Secure Protocols through Cross-Layer Design Techniques. 京都大学, 2019, 博士(情報学)

ISSUE DATE:

2019-05-23

URL:

https://doi.org/10.14989/doctor.k21975

（ 続紙 １ ）

| 京都大学 | 博士（情報学） | 氏名 | 辺　松（Song Bian） |
|---|---|---|---|
| 論文題目 | Realizing Homomorphic Secure Protocols through Cross-Layer Design Techniques（クロスレイヤ設計による準同型暗号プロトコルの実現） | | |

（論文内容の要旨）

本論文は、クラウド・コンピューティング等の外部委託された計算資源を用いる環境下において、データを暗号化したまま計算することで安全な情報処理を行うプロトコルを、複数の設計階層の連携により効率よく実現する手法に関する研究である。特に、Learning with Errors（LWE）問題と整数環上のLWE問題であるring-LWE（環LWE）問題にもとづく準同型暗号に着目し、専用の計算ハードウェアを構成することで計算時間や消費エネルギーの効率化を目指す点に特徴がある。本論文は、以下の全７章から成っている。

第１章は序論であり、現在および今後の計算環境における秘密情報保護の動向と、その中で準同型暗号を用いる安全な暗号プロトコルが果たす役割について概要を述べている。暗号化されたデータに対し計算を実行するプロトコルの設計に対する階層を定義するとともに、既存の具体的構成例に対する議論を通じて本研究の目的と本研究の概要を示している。

第２章では、本論文で用いられる暗号技術、暗号プロトコルの概要と既存研究について理論的、手続き的側面から説明している。鍵交換スキームの構成に代表されるLWE問題の暗号技術への応用について示すとともに、特に本論文で中心的に扱われるLWE問題および環LWE問題による準同型暗号を用いた具体的なプロトコル構成について既存研究の要点を述べている。

第３章では、LWE問題と環LWE問題ベースの鍵共有アルゴリズムを効率的に実行可能な演算器を設計、比較している。(環)LWE問題において中心となるベクトルと行列に関する計算をFPGA上のDSPを用いて実行する既存アーキテクチャに対し、特定用途向け集積回路上に専用ハードウェアとして実装した数論変換による提案多倍長整数乗算器は、約40倍の高速化と10倍以上のエネルギー効率を実現した。また、具体的なアプリケーションでの処理時間、メモリ帯域幅、消費エネルギーを比較した。サーバとクライアントの計算負荷を非対称とする場合、ハードウェア実装を考慮した最適化によりLWE問題ベースの鍵共有アルゴリズムを、一般に高効率と考えられている環LWEと同等以下のエネルギー効率で実現できる場合があることを明らかとした。

第４章では、LWE問題にもとづく準同型暗号の計算において用いるノイズは演算誤差と区別ができないという着想のもとに、準同型暗号の復号をApproximate Computingの考え方を用いて効率化するハードウェア実装手法を提案している。ここでApproximate Computingとは、論理回路による数値の近似およびその演算における許容誤差を大きくすることでハードウェア量を削減する近似計算手法である。近似誤差の偏りが小さい近似乗算器を用いる場合について、演算により蓄積する誤差をノイズの一部とみなし、暗号パラメータと組み合わせた際の復号失敗確率を高速に推定する方法を考案することで、アプリケーションに応じた専用回路の設計を可能とした。これにより、暗号サイズ、計算時間、回路面積の削減と、エネルギー効率の改善を同時に達成できることを示した。

第５章では、加法準同型暗号の一つであるPaillier暗号を利用して、ベイズフィルタを用いるスパムメール判定を委託された計算資源上で安全に実行するアプリケーションについて、そのプロトコルと、効率の良い実装方法を示した。準同型暗号による

フィルタ処理をハードウェア構造を考慮しつつ単純化することで、加法準同型性のみを用いる安全かつ効率的なアーキテクチャを示した。Karatsuba法を再帰的に適用して効率化した多倍長整数乗算器をパイプライン化して用いるとともに、複数単語を同時に評価できるようパッキングする手法を組み合わせた専用ハードウェアの実装例では、暗号化されたままの平均的な長さの電子メールのフィルタリングを、プロセッサに対し約30倍高速化できることが示されている。

第６章では、畳み込みニューラルネットワークによる推論をLWE問題にもとづく暗号化により安全に行うシステムを提案した。暗号化された入力データに対し畳み込み層や全結合層で行なわれる計算を、周波数領域での要素積の計算に置き換えて処理量を軽減する手法を提案した。同時に、量子化された係数を用いる演算で蓄積される分布形状が明らかでない誤差の上界を、極値推定のためのモンテカルロ法を応用して高速かつ精度よく求める手法を示した。この手法を適用してニューラルネットワークの各層で蓄積される誤差を見積もることにより、ネットワーク層ごとの暗号パラメータを誤差に応じて決定することが可能となり、計算時間等、推論の効率と得られる精度のトレードオフを示した。

第７章は結論であり、本論文で得られた結果を総括的にまとめている。

注)論文内容の要旨と論文審査の結果の要旨は１頁を３８字×３６行で作成し、合わせて、３,０００字を標準とすること。
論文内容の要旨を英語で記入する場合は、４００～１,１００wordsで作成し
審査結果の要旨は日本語５００～２,０００字程度で作成すること。

（続紙　２　）

（論文審査の結果の要旨）

本論文は、暗号化が施されたデータに直接情報処理を実行する秘匿計算を対象として、その暗号プロトコルとそれを実行するハードウェアの設計方法を提案している。特に格子問題にもとづく準同型暗号に着目し、秘匿計算のアプリケーション、暗号アルゴリズム、およびハードウェアとして抽象化された複数の設計階層を考慮する設計により、安全性を従来と同等に保ちながら、計算時間や消費エネルギー、通信バンド幅削減等の性能向上が実現できることを、理論的検討と数値シミュレーションを通じて検証している。本論文で得られた成果は以下の通りである。

1. 格子問題にもとづく暗号アルゴリズムに特化した近似乗算器とその活用方法を提案した。提案手法では、暗号アルゴリズムに適する近似乗算器を提案し、近似により生じる誤差が暗号アルゴリズム中で与えられているノイズに加算されることの影響を評価する方法を与え、復号に影響を与えない最大の近似ビット数を得る。提案された近似演算器の適用と暗号パラメータの決定により、既存のハードウェアに組み込まれている汎用乗算器を用いて演算を行う従来手法に対し、回路面積と演算に必要なエネルギーを大幅に削減できることを示した。

2. 暗号化されたメール本文がスパムであるか否かを判定する単純ベイズ分類器が、加法準同型暗号のみを用いるアルゴリズムにより現実的な計算時間で実現可能であることを示した。本提案により、その検索内容であるメール中の単語をサーバ側に明かすことなくメールフィルタリングの実行を委託する計算が可能となる。アルゴリズム面では、フィルタに用いる係数の量子化と複数単語を並列に演算実行できる暗号への埋め込み方法を提案し、ハードウェア面では、多倍長整数演算に適する効率的な演算器の実装を示した。実メールデータベースを用いた性能評価により、プロセッサおよび専用ハードウェアを用いるいずれの従来実装に対しても、大幅な高速化が達成された。

3. 畳み込みニューラルネットワークによる推論を格子問題にもとづく暗号化により安全に行うプロトコルを提案した。ニューラルネットワーク中で特に計算量の大きい、準同型暗号による畳み込み層と全結合層の計算高速化手法を示した。秘密分散法を応用し、またフーリエ変換と同様の方法により畳み込み演算をより軽量な要素積の計算に帰着させて、計算量を削減した。さらに、畳み込み層と全結合層に対して、係数の量子化と蓄積される誤差評価にもとづいて暗号パラメータを決定する方法を与えた。具体例を用いた実装評価により、計算時間と通信帯域幅が大幅に削減できることを示した。

以上、本論文では、格子暗号を用いて安全性と効率性を両立する計算環境を、暗号プロトコルからハードウェアまでの設計階層をまたがる最適化を通じて構築する方法を提案している。また提案手法の有効性を、具体的な実装例をもって実証している。本論文の内容は、学術上、応用上ともに寄与するところが少なくない。よって本論文は博士（情報学）の学位論文として価値あるものとして認める。また平成３１年４月１８日に実施した論文内容とそれに関連した試問の結果、合格と認めた。

注）論文審査の結果の要旨の結句には、学位論文の審査についての認定を明記すること。
更に、試問の結果の要旨（例えば「平成　年　月　日論文内容とそれに関連した口頭試問を行った結果合格と認めた。」）を付け加えること。

Webでの即日公開を希望しない場合は、以下に公開可能とする日付を記入すること。
要旨公開可能日：　令和元年１１月３０日以降